CLAIMS

1. A method for generating a non-linear output stream from a linear feedback shift register (LFSR), comprising:

shifting a plurality of bits through the LFSR, wherein the LFSR is structured in accordance with a recurrence relation;

performing modular multiplications upon the plurality of bits, wherein the modular multiplications are implemented through pre-computed look-up tables, wherein the pre-computed look-up tables are computed using an irreducible polynomial; and

performing a non-linear operation on a selected portion of the shifted plurality of bits, wherein the selected portion is selected so that the pairwise distances between elements in the selected portion are distinct values.

2. The method of Claim 1, wherein the non-linear operation is defined as $V_n = (S_n + S_{n+5}) \times (S_{n+2} + S_{n+12})$, where the non-linear operation is defined over $GF(2^8)$.

3. The method of Claim 1, wherein the non-linear operation is a stuttering operation.

4. The method of Claim 1, further comprising the step of initializing the LFSR before shifting the plurality of bits, wherein initializing the LFSR comprises:

adding a byte of a secret key to an element in the LFSR; and

adding a byte of a secondary key to the LFSR for each frame of data that passes through the LFSR.